Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 215 - 230

Strengthening Differential and Linear Attacks using Virtual Isomorphisms

A. G. Rostovtsev and A. F. Suprun
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 01 April, 2014)

The ciphers $y = C(x,\ k)$ and $\mathbf{y} = \mathbf{C}(\mathbf{x}, \mathbf{k})$ are isomorphic if there is a computable in both directions map $y \leftrightarrow \mathbf{y}$, $x \leftrightarrow \mathbf{x}$, $k \leftrightarrow \mathbf{k}$. The cipher is vulnerable to an attack if the isomorphic cipher is vulnerable to it. If φ is a substitution and T is an encryption operator, then $\mathcal{T} = \varphi T \varphi^{-1}$ is a cipher isomorphism. For cryptanalysis it is reasonable to choose substitution φ in such a way that it has a lot of fixed points. It is shown that byte substitution φ can have no more than 130 fixed points. Isomorphic AES (IAES) is proposed where the only non-linear operation is an isomorphic image of the XOR operation. On average, maximum probabilities of IAES differentials are 8.5 times higher in comparison with the original whereas dominance of the linear sum is increased by 3 times. IAES has differentials with zero output difference and probability 1, which slows down replication of active non-linearities and decreases complexity of an attack. Presumably, resistance of AES to linear and differential attacks can be twice reduced by magnitude in comparison with the generally accepted estimates.

PACS numbers: 89.70.-a
Keywords: information security, monitoring system

1. Introduction

The papers [1, 2] suggest using a method of virtual isomorphisms for cryptanalysis. The ciphers $y = C(x, k)$ and $\mathbf{C} = (\mathbf{x}, \mathbf{y})$ are isomorphic if there is a computable in both directions map $y \leftrightarrow \mathbf{y}$, $x \leftrightarrow \mathbf{x}$, $k \leftrightarrow \mathbf{k}$. Usually, cipher C is real, but its isomorphic image $\mathbf{C}$ is virtual and only exists in a cryptanalyst's imagination. Isomorphism is not an equivalency since no transitivity is provided: computable map composition is not necessarily computable (analogy: it is easy to compute a key for one encryption cycle, but it is difficult to do it for 10 ones). In [1, 2] the following assumption has been proved.

Theorem 1. *A cipher is vulnerable to some attack if and only if the isomorphic cipher is vulnerable to the same attack.*

That is why the search for vulnerability of the cipher can be substituted with the search for a suitable isomorphism. If φ is a substitution and T is a cycle encryption function, then $\mathcal{T} = \varphi T \varphi^{-1}$ is a cipher isomorphism.

Two substitutions are conjugated if and only if they have the same cycle type [3]. So a non-linear substitution defined by inversion in the finite field, is conjugated with the affine substitution, defined by one or several bits inversion.

Isomorphism of ciphers, defined by conjugation [1] is not practical: in the isomorphic cipher all operations, carried out in one cycle of encryption, apart from one become non-linear. Conjugate substitution φ was chosen in such a way so that it would have a lot of fixed points.

The most popular methods to compute unknown parameters are linear [4] and differential [5] ones, which require a lot of plaintext and ciphertext. Apart from this, there are algebraic methods [6, 7] based on solving some systems of algebraic equations that describe a map and require just a few plaintexts and ciphertexts. It is possible to combine these methods [8].

Let n-bit substitution S change an input

vector $\mathbf{x} = (x_1, \ldots, x_n)$ into an output vector $\mathbf{y} = (y_1, \ldots, y_n)$. If x_i, $y_i$are independent binary variables then linear over the field $\mathbb{F}_2$ function $\sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} b_i y_i$, a_i, $b_i \in \mathbb{F}_2$ takes value 0 and 1 with the same frequency. However, if x_i, y_i are inputs and outputs of the substitution, probabilities $P(0)$, $P(1)$ of 0 and 1 can differ from 0.5. The remainder $P(0) - 0.5$ is called dominance. Linear analysis is based on search for such non-constant linear functions with maximum absolute dominance of linear sums (ADLS). The operation of addition with a constant does not change the linear sum. The linear operation of diffusion as a result of distribution law does not change the value of dominance but does change the type of the linear sum. Thus, it is possible to obtain, for the map as a whole, linear sums of input text, key and output text bits plus probability that this sum will equal 0. If the number of known texts is rather big, unknown parameters are computed through solving a system of linear equations. The resulting dominance is proportional to the product of factors. The weakest substitutions are the ones that have linear sums with dominance ± 0.5.

Let $\mathbf{x}, \mathbf{x}'$ be a pair of binary vectors, $\mathbf{y} = S(\mathbf{x})$, $\mathbf{y}' = S(\mathbf{x}')$. Let us mark $\Delta\mathbf{x} = \mathbf{x} + \mathbf{x}'$, $\Delta\mathbf{y} = \mathbf{y} + \mathbf{y}'$, at this $\Delta\mathbf{y} = 0$ if and only if $\Delta\mathbf{x} = 0$. Differential analysis is based on the fact that probabilities of differentials $(\Delta\mathbf{x}, \Delta\mathbf{y})$ are distributed non-uniformly. The operation of addition with the key keeps the differential and its probability, the diffusion operation changes the type of the differential but maintains its probability. Computation of unknown parameters reduces to search for most probable differentials for a map as a whole. Probability of the resulting differential equals the product of probabilities of factor differentials. The weakest substitutions are the ones that have differentials with probability 1.

To resist linear and differential analysis, substitutions are chosen so that both maximum probability of the substitution differential and maximum absolute dominance value for the substitution can minimized.

The placecountry-region USA encryption standard called AES [9] uses such a substitution defined by the inversion in field $\mathbb{F}_{256}$. Maximum probability of the differential equals 4/256, maximum dominance of the linear sum is 16/256. This substitution has two fixed points and 127 cycles of length 2, so it can be suggested approximately that all cycles of this substitution have length 2 (accuracy of such approximation is 2^{-7}). Then the inversion in field $\mathbb{F}_{256}$ is accompanied almost everywhere by the substitution defined as addition with constant. Presumably, complexity of a differential and linear attack on AES exceeds the complexity of scanning the keys.

This paper shows that conjugate substitution φ can have 130 fixed points and this assessment cannot be improved. An isomorphism has been proposed with the use of four auxiliary substitutions wherein isomorphic AES (IAES) image has only one non-linear operation – XOR operation image. At that, probabilities of IAES differentials are raised by 8.5 times in comparison with the original cipher whereas dominance of linear sums has been tripled. Rough estimation shows that, since probability of the differential grows from p to $\sqrt{p}$, which the proposed isomorphism accepts, the AES strength halves by the order of magnitude. This creates prerequisites for practical attacks on AES with the use of a virtual isomorphism technique.

2. Algebraic basis

If S, T are elements of symmetric group G, then map σ_S: $T \to STS^{-1}$ is conjugation. Conjugation is equivalency and divides group G by classes of conjugate elements. If S runs the entire symmetric group, we get a class for T.

Let G be a subgroup of the symmetric group of n-bit substitutions, generated by two or several substitutions, and x be the substitution input. The orbit of element x is a set of n-bit words into which x can be transformed by

substitutions from G. Ownership of two words by one orbit is equivalency. So the set of n-bit words is divided into non-crossing orbits (in relation to group G). If group G is cyclic and formed by one substitution, the orbits are cycles of the substitution.

Each substitution can be defined by sets of cycles. If $l_1, \ldots, l_r$ are lengths of all substitution cycles, then $\sum_{i=1}^{r} l_i = 2^n$. The set of numbers $(l_1, \ldots, l_r)$, $l_i \leqslant l_{i+1}$, $\sum l_i = 2^n$, is called a cycle type of the substitution. Substitutions are conjugate if and only if they have the same cycle type [3].

Substitution S is called affine one if it is defined by equation $\mathbf{y} = L\mathbf{x} + \mathbf{c}$, where L is an invertible over $\mathbb{F}_2$ matrix (when $\mathbf{c} = 0$ the substitution is linear). Affine substitutions form a subgroup of the substitution group. Substitutions S, T are affinely equivalent if there is a relation $S = ATB$, where A, B are affine substitutions. Affine equivalency is effectively identified [10].

Let $\mathbf{y} = T(\mathbf{x})$ be an arbitrary map of a set of n-bit words in themselves. This map can be defined through use of interpolating polynomials over the field of characteristic 2. Such polynomials create a finite ring. The Zhegalkin polynomial ring is usually used:
$\mathbf{G}_n[\mathbf{x}] = \mathbb{F}_2[x_1, \ldots, x_n]/({x_1}^2 + x_1, \ldots, {x_n}^2 + x_n)$.

The Zhegalkin polynomial ring is finite (as a result, it is Artin) and has zero Krull dimension [11]. In it the product of ideals coincides with their intersection. Each ideal is expanded into prime factors. The prime ideal is maximal and consists of polynomials turning into 0 at this set of variables. There are altogether 2^n prime ideals.

A prime ideal is defined by one polynomial, for example, $1 + x_1 \ldots x_n$. That is why each ideal of the ring $\mathbf{G}_n[\mathbf{x}]$ can be defined by one polynomial. The set of vectors $\mathbf{x}$ of n bit length forms the affine space $\mathbb{A}^n$. At this $\mathcal{M}^2 = \mathcal{M}$, the zero ideal corresponds to $\mathbb{A}^n$, the unit ideal corresponds to an empty set.

Automorphism of the ring $\mathbf{G}_n[\mathbf{x}]$ keeps constants and transforms a prime ideal into a prime ideal (supposing a prime ideal gets mapped into the product of different prime ideals, inversion gets upset). Every permutation of prime ideals is an automorphism of the ring $\mathbf{G}_n[\mathbf{x}]$ and inversely, every automorphism is defined by some substitution. Since there is a bijection between the set of space points $\mathbb{A}^n$ and set of prime ideals, the group of automorphisms is isomorphic towards the group of set permutations from 2^n elements. Any permutation is defined by a set of polynomials from $\mathbf{G}_n[\mathbf{x}]$. Map of the polynomial ring is called regular if it is defined by a set of polynomials. If there is also an inverse map, it is called biregular. So, all automorphisms $\mathbf{G}_n[\mathbf{x}]$ are biregular.

Probabilities of differentials and linear sums of n-bit substitution can be represented as a square matrix of size 2^n [12]. Rows and columns of the matrix of differentials $(\Delta\mathbf{x}, \Delta\mathbf{y})$ correspond to sets $\{\Delta\mathbf{x}, \Delta\mathbf{y}\}$. Elements of the matrix correspond to the number of appearance of this differential if the substitution input runs the entire set of 2^n values. Similarly, dominance of linear sums $\sum_i a_i x_i + \sum_j b_j y_j$ are defined by the matrix with rows corresponding to $\sum_i a_i x_i$, and columns corresponding to $\sum_j b_j y_j$. The elements of the matrix conform to the number of this linear sum execution if the substitution input runs the entire set of 2^n values minus 2^{n-1}.

Any substitution is defined by the Zhegalkin polynomial system, i.e. by sharable zeros of the polynomial set. The polynomial set defines ideal A, the set of the ideal's zeros is a variety $V(\mathcal{A})$ and inversely, any variety as a set of points explicitly defines some ideal. Thus, every substitution is explicitly defined by the ideal and variety.

Any image of finite Boolean sets is defined by the ideal and variety. The ideal and variety of substitution S correspond to two substitutions S, S^{-1} at least.

Let us mark $\oplus$ the symbol of ideal addition. It is obvious that $\mathcal{A} \oplus \mathcal{B} \supseteq \mathcal{A}$, $V(\mathcal{A} \oplus \mathcal{B}) \subseteq V(\mathcal{A})$ for ideals $\mathcal{A}$ and $\mathcal{B}$.

Let us define probability of a differential $\Delta\mathbf{x} = (x_{i_1}, ..., x_{i_k})$ of an arbitrary ideal $\mathcal{A} \subset \mathbf{G}_n[\mathbf{x}]$. Let $\mathcal{A} = (f(\mathbf{x}))$. Let us mark the formal partial derivative by x_i as $D(f, x_i)$, introduce relation $D(f, \{x_i, x_j\}) = D(f, x_i) + D(f, x_j) + D(D(f, x_i), x_j)$;

and further on by induction: $D(f, \{x_{i_1}, \; ldots, \; x_{i_l}\}) = D(D(f, \{x_{i_1}, \; \ldots, \; x_{i_{l-1}}\}), \; x_{i_l})$. It is obvious that $D(f, \{x_{i_1}, ..., x_{i_k}\})$ is a polynomial and, consequently, defines the ideal as well. Probability of the differential $\Delta x = (x_{i_1}, \; \ldots, \; x_{i_k})$ of an ideal $\mathcal{A} = (f)$ equals

$$\frac{\#V\left((f)\right) \oplus \left(D\left(f, \{x_{i_1}, \; \ldots, \; x_{i_k}\}\right)\right))}{\#V((f))}.$$

This definition extends the one for the differential of a substitution. Thus, it is possible to calculate any map probability of the s-bit words set into the set of t-bit words.

Similarly, it is possible to define non-linearity of an ideal as the Hamming distance between the polynomial, predetermining the principal ideal, and the set of affine functions, at this, differences are added only by the variety of the ideal.

3. AES isomorphisms

Let x, y, k be respectively the plaintext, cipher text and key of cipher C, and let $\mathbf{x}, \mathbf{y}, \mathbf{k}$ be respectively the plaintext, cipher text and key of cipher $\mathbf{C}$. Isomorphism of ciphers C,$\mathbf{C}$ is a computable in either direction, invertible map $y \leftrightarrow \mathbf{y}$, $x \leftrightarrow \mathbf{x}$, $k \leftrightarrow \mathbf{k}$. Thus the relation $y = C(x, k)$ is met if and only if there is the relation $\mathbf{y} = \mathbf{C}(\mathbf{x}, \mathbf{k})$. Ciphers C, $\mathbf{C}$ are called isomorphic if there is an isomorphism between them ($C \cong \mathbf{C}$). Cipher C is vulnerable to some cryptanalysis method if and only if isomorphic cipher $\mathbf{C}$ is vulnerable towards the same cryptanalysis method.

The technique of virtual isomorphisms can be illustrated with the example of the USA AES cryptographic standard [9].

AES standard has 10, 12 or 14 encryption cycles, the block length is 128 bits, the key length is 128, 192 or 256 bits. The following operations are performed in every cycle.

1. A block is divided into bytes and fixed substitution $z = S(x)$ of bytes is made (probabilities of differentials and ADLS do not exceed 2^{-6}). The substitution is defined as a composition of operation U raising to power 254 in the finite field $\mathbb{F}_{256} = \mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1)$ and an affine substitution. The result of raising to the power is represented as 8-bit vector $\mathbf{y}$ over $\mathbb{F}_2$, and it is assumed that $\mathbf{z} = L\mathbf{y} + \mathbf{c}$, where every element $\mathbf{c}$ is a trace of the row of matrix L as an element of field $\mathbb{F}_{256}$ in field $\mathbb{F}_2$,

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \; \mathbf{c} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

   Let us mark $M(\mathbf{x}) = L\mathbf{x} + \mathbf{c}$. Substitution M consists of cycles with length 4. Maximum probability of substitution differential S equals $4/256$, maximum dominance of the linear sum is $16/256$.

2. A diffusion operation, which can be defined as matrix W with size 16×16 over field $\mathbb{F}_{256}$, affecting a 16 element vector.

$$W = \begin{pmatrix}
t & 0 & 0 & 0 & 0 & 1+t & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & t & 0 & 0 & 0 & 0 & 1+t & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & t & 0 & 0 & 0 & 0 & 1+t \\
1+t & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & t \\
0 & 0 & 0 & 1 & t & 0 & 0 & 0 & 0 & 1+t & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & t & 0 & 0 & 0 & 0 & 1+t & 0 \\
0 & 0 & 0 & 1+t & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & t & 0 \\
0 & 0 & 0 & t & 1+t & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & t & 0 & 0 & 0 & 0 & 1+t & 0 & 0 \\
0 & 0 & 1+t & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & t & 0 & 0 \\
0 & 0 & t & 0 & 0 & 0 & 0 & 1+t & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & t & 1+t & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1+t & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & t & 0 & 0 & 0 & 0 & 1+t & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & t & 0 & 0 & 0 & 0 & 1+t & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & t & 1+t & 0 & 0 & 0
\end{pmatrix}.$$

3. An operation of addition with the cycle key (XOR). This operation can be united with addition of bytes in a diffusion map.

Thus, AES is described in terms of substitution of a byte, the product by matrix, addition of bytes.

Each byte can be represented as a binary vector in the basis $[1, t, t^2, \ldots, t^7]$. Elements 0, 1, t, $1 + t$ of matrix W correspond to the matrixes over field $\mathbb{F}_2$ with size of 8*8: zero, identity E,

$$L_t = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}$$

and $L_{t1} = L_t + E$. At this, $L_t L_{t1} = L_{t1} L_t$, but conditions $M(L_t(x) = L_t(M(x))$, $M(L_{t1}(x) = L_{t1}(M(x))$ are impossible for none of x. Matrix W can be seen as a block one over $\mathbb{F}_2$, containing blocks of 4 types.

Next, we will see the AES substitution as an inversion in a finite field and operation M as a constituent of a diffusion map. At this, the zero block of matrix W remains zero due to the relation $0M = 0$. The identity block of matrix W transforms into affine substitution M. Block L_t transforms into the affine substitution $L_t(M\mathbf{x} + \mathbf{c}) = L_t M\mathbf{x} + L_t\mathbf{c}$. Block $L_t + E$ transforms into the affine substitution $(E + L_t)(M\mathbf{x} + \mathbf{c}) = (M + L_t M)\mathbf{x} + (E + L_t)\mathbf{c}$.

Substitution U, defined as an inversion in the finite field consists of 127 cycles of length 2 and two fixed elements $\{0, 1\}$. Let T be a substitution where $T(1) = 0$, $T(0) = 1$, $T(x) = U(x)$ under $x \neq 0, 1$. Then the relation $U(x) = T(x)$ is executed with high probability $1 - 2^{-7} = 0.992$. Substitution T consists only of length 2 cycles and so it is conjugated with the affine substitution that consists of length 2 cycles:
T= {1, 0, 141, 246, 203, 82, 123, 209, 232, 79, 41, 192, 176, 225, 229, 199, 116, 180, 170, 75, 153, 43, 96, 95, 88, 63, 253, 204, 255, 64, 238, 178, 58, 110, 90, 241, 85, 77, 168, 201, 193, 10, 152, 21, 48, 68, 162, 194, 44, 69, 146, 108, 243, 57, 102, 66, 242,

53, 32, 111, 119, 187, 89, 25, 29, 254, 55, 103, 45, 49, 245, 105, 167, 100, 171, 19, 84, 37, 233, 9, 237, 92, 5, 202, 76, 36, 135, 191, 24, 62, 34, 240, 81, 236, 97, 23, 22, 94, 175, 211, 73, 166, 54, 67, 244, 71, 145, 223, 51, 147, 33, 59, 121, 183, 151, 133, 16, 181, 186, 60, 182, 112, 208, 6, 161, 250, 129, 130, 131, 126, 127, 128, 150, 115, 190, 86, 155, 158, 149, 217, 247, 2, 185, 164, 222, 106, 50, 109, 216, 138, 132, 114, 42, 20, 159, 136, 249, 220, 137, 154, 251, 124, 46, 195, 143, 184, 101, 72, 38, 200, 18, 74, 206, 231, 210, 98, 12, 224, 31, 239, 17, 117, 120, 113, 165, 142, 118, 61, 189, 188, 134, 87, 11, 40, 47, 163, 218, 212, 228, 15, 169, 39, 83, 4, 27, 252, 172, 230, 122, 7, 174, 99, 197, 219, 226, 234, 148, 139, 196, 213, 157, 248, 144, 107, 177, 13, 214, 235, 198, 14, 207, 173, 8, 78, 215, 227, 93, 80, 30, 179, 91, 35, 56, 52, 104, 70, 3, 140, 221, 156, 125, 160, 205, 26, 65, 28}.

It is convenient to choose the affine substitution as conjugate image $\mathcal{T}$ of substitution T (for example, M^2 or addition with constant). Conjugate substitution $\mathcal{T}$ has probability differentials 1 and linear sums with absolute dominance 0.5. Substitution T has maximum probabilities of differentials $4/256$ and dominance of linear sums $16/256$.

Let us define distance $d(S_1, S_2)$ between two n-bit substitutions S, T as a number of inputs, for which $S_1(x) \neq S_2(x)$. The affine substitution has differentials and linear sums with probability of 0 or 1. The distance between this substitution $S(x)$ and a group of affine substitutions $\mathrm{Aff}\,(x)$ equals $\min(d(S, A))$, if $\mathcal{A}$ runs the entire group Aff. Typically, the closer the substitution is to the affine one in terms of the stipulated remainder, the bigger the probability of differentials is.

If the stipulated affine substitution is an identity one, the distance between conjugate substitution φ and the unit substitution equals to the number of substitution points φ so that $\varphi(x) \neq x$. That is why to approximate the conjugate substitution to the affine substitution it is desirable to provide a bigger number of fixed points.

Let G be a group forcing on set M. Let us mark $\mathrm{Orb}(x, G)$ the orbit of element $x \in M$ in relation to group G. Let us choose substitution φ so that it has maximum number of fixed points. For this, let us divide the set of bytes into orbits in relation to group $\langle T, \mathcal{T}\rangle$, generated by substitutions T and $\mathcal{T}$.

Theorem 2. *Let S_1, S_2 be substitutions forcing on n-bit words and consisting only of length 2 cycles and let $\langle S_1, S_2\rangle$ be the group generated by these substitutions. Then Orb(x, $\langle S_1, S_2\rangle$) has an even length.*

Proof Since ${S_1}^2 = {S_2}^2 = E$ (identity substitution) the group consists of substitutions $\{E, S_1, S_2, S_1 S_2, S_2 S_1, S_1 S_2 S_1, S_2 S_1 S_2, S_1 S_2 S_1 S_2, \dots\}$. According to the condition, the orbit length is not less than 2. Let us assume that some orbit has length 3. Without loss of generality, one can consider that the orbit of element x includes $S_1(x)$. Then $S_1 S_2 S_1(x) = x \Rightarrow S_1 S_2(x) = S_1(x)$, from which $S_2(x) = x$, which is impossible. Likewise it is proved that the orbit length cannot equal 5, 7, etc. ■

Consequence 1.

Orbits of group $\langle T, \mathcal{T}\rangle$ have an even length.

It is directly tested that out of 255 possible substitutions $\mathcal{T}$, defined by inversions of several bits, only the inversion of the least significant bit jointly with substitution $\mathcal{T}$ gives two orbits of length 2, whereas other orbits have length 6. Other substitutions $\mathcal{T}$ give orbits of bigger length, which limits the choice of conjugate substitution φ.

If the orbit has length 2 then both elements of the orbit can be fixed points of substitution φ. Indeed, if the orbit consists of elements (a, b), then $T(a) = b$, $T(b) = a$, $\mathcal{T}(a) = b$, $\mathcal{T}(b) = a$. Since $\varphi T \varphi^{-1} = \mathcal{T}$ it can be assumed that $\varphi(a) = a$, $\varphi(b) = b$.

Theorem 3. *Let n-bit substitutions S_1, S_2 consist of cycles of length 2 and the orbit length of element a in relation to group $\langle S_1, S_2\rangle$ is bigger than 2. The following conclusions are true.*

1. *The orbit of an element in relation to group $\langle S_1, S_2\rangle$ coincides with the orbit of the same*

element in relation to any group $\langle S_1, S_1S_2\rangle$, $\langle S_1, S_2S_1\rangle$, $\langle S_2, S_1S_2\rangle$, $\langle S_2, S_2S_1\rangle$.

2. *The orbit of element a can be written down in a cyclic type* $(a, S_1(a), S_2S_1(a), S_1S_2S_1(a), S_2S_1S_2S_1(a), \ldots)$.

3. *The orbit length of element a in relation to the group* $\langle S_1, S_2\rangle$ *equals the duplicate cycle length of element a in substitution* S_2S_1.

4. *There is such a conjugate substitution* φ *that* $S_1 = \varphi S_2\varphi^{-1}$, *which keeps the elements fixed on either all even or all odd positions of the orbit according to clause 2.*

5. *There is no conjugate substitution with the number of fixed points of the orbit bigger than half of the orbit.*

6. *If* $S_1 = \varphi S_2\varphi^1$ *and* φ *keeps elements fixed on either even or odd positions of the orbit, then* $Orb(x, \langle S_1, S_2\rangle) = Orb(x, \langle S_1, S_2, \varphi\rangle)$ *for all x.*

Proof (1) In virtue of equation $S_1{*}S_1S_2 = S_2$ substitutions S_1, S_1S_2 can be considered as the ones forming groups $\langle S_1, S_2\rangle$. From equation $S_2S_1{*}S_1 = S_2$ it follows that $\langle S_1, S_2\rangle = \langle S_1, S_2S_1\rangle$. Similarly it is proved that $\langle S_1, S_2\rangle = \langle S_2, S_1S_2\rangle = \langle S_2, S_2S_1\rangle$.

(2) and (3) Let the cycle length of element a for substitution S_2S_1 equal k. Then $k > 1$ since from conditions $S_2S_1(a) = a$ and ${S_1}^2(a) = a$ it follows that $S_1(a) = S_2(a)$, and the orbit consists of two elements, which goes against the condition. If we multiply equation $(S_2S_1)^k(a) = a$ by S_2 on the left, we obtain $(S_1S_2)^{k-1}S_1(a) = S_2(a)$. So, the mentioned cycle contains $S_2(a)$. Similarly, $(S_1S_2)^{k-1}(a) = S_2S_1(a)$, $(S_1S_2)^{k-2}S_1(a) = S_2S_1S_2(a)$. So, the cycle mentioned in clause 2 contains a, $S_1(a)$, $S_2(a)$, $S_1S_2(a)$, $S_2S_1(a)$, ..., i.e. the entire orbit of element a. Elements of this cycle on odd positions correspond to the substitution cycle S_2S_1. Since the orbit length is even, it equals the duplicate cycle length of the substitution S_2S_1.

(4) To calculate substitution φ let $\varphi(a) = a$. Then from the equation $S_1(a) = \varphi S_2\varphi^{-1}(a) = \varphi(S_2(a))$ we find $\varphi(S_2(a))$. Then, let $\varphi(S_2S_1(a)) = S_2S_1(a)$ (this is a fixed point) and find $\varphi(S_2S_1S_2(a))$, etc. We obtain fixed elements of substitution φ on all odd positions of the cycle according to clause 2. Similarly, it is possible to make the elements fixed on all even positions of the cycle.

(5) Supposing we have managed to make all the elements on odd positions and one element on an even position fixed. Without loss of generality it can be assumed that it is element $S_1(a)$. Then conditions of fixity of points a, $S_1(a)$ in substitution φ result in equation $S_2S_1(a) = a$, which contradicts the condition of the theorem (orbit length of element a is bigger than 2).

(6) The proof results from the fact that if $y \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$ and $\varphi(y) = y$, then $\varphi(S_2(y)) = S_1(y)$, and also $S_1(y) \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$, $S_2(y) \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$, i. e. the input and output of substitution φ lie in $\mathrm{Orb}(x, \langle S_1, S_2\rangle)$. ■

The experiment demonstrates that if substitution $\mathfrak{T}$ is an inversion of the least significant bit, the two orbits of bytes in relation to group $\langle T, \mathfrak{T}\rangle$ have length 2: {{0, 1}, {188, 189}}, and other 42 orbits have length 6: {2, 3, 246, 247, 140, 141}, {4, 5, 82, 83, 202, 203}, {6, 7, 209, 208, 122, 123}, ..., {214, 215, 234, 235, 227, 226}. If it is not the least significant bit, but other sets of bits that get inverted, the number of orbits diminishes considerably whereas the orbit length grows.

Theorem 3 results in the following assumption.

Consequence 2.
1. For substitution T and inversion of the least significant bit $\mathfrak{T}$ there are 2^{42} conjugate substitutions φ, complying with equation $\mathfrak{T} = \varphi T\varphi^{-1}$ and having 130 fixed points.
2. There are no other substitutions $\mathfrak{T}$ defined as an inversion of one or several bits for which conjugate substitution φ, complying with equation $\mathfrak{T} = \varphi T\varphi^{-1}$, would have 130 or more fixed points.

Theorem 4. *There is no affine substitution* $\mathfrak{T}$

where $\mathfrak{T}^2 = E$ *and* $\mathfrak{T}$ *has only two fixed points.*

Proof Let us examine such substitution $\mathfrak{T}(\mathbf{x}) = L\mathbf{x} + \mathbf{c}$. Let $L\mathbf{x}_1 + \mathbf{c} = \mathbf{x}_1$, $L\mathbf{x}_2 + \mathbf{c} = \mathbf{x}_2$ be fixed points. Then $L(\mathbf{x}_1 + \mathbf{x}_2) = \mathbf{x}_1 + \mathbf{x}_2$ is the only non-zero solution, so it is possible to consider that $\mathfrak{T} = L$. Let $L\mathbf{a} = \mathbf{a}$ be the only non-zero solution. Then $L(\mathbf{a} + \mathbf{x}) = L\mathbf{a} + L\mathbf{x} = \mathbf{a} + L\mathbf{x}$. Without loss of generality it can be assumed that $\mathbf{a} = (1, 0, \ldots, 0)$. Then the first row and first column of matrix L equal $\mathbf{a}$. Let us mark 7*7 the block of matrix L, which consists of other elements, like L_7. Then the equation $L_7\mathbf{b} = \mathbf{b}$ is impossible for non-zero $\mathbf{b}$ (otherwise L will have 4 fixed elements). Consequently, the matrix $L_7 + E$ is invertible and ${L_7}^2 = E$. But then the matrix $(L_7 + E)^2$ has to be invertible, too. We have contradiction $(L_7 + E)^2 = {L_7}^2 + E = 0$. ■

Consequence 3. There is no affine substitution, conjugate with the inversion in $\mathbb{F}_{256}$.

4. Isomorphic AES for four auxiliary byte substitutions

Conjugate AES has a linear operation of substitution, non-linear operations of diffusion (substitution images M, L_t, L_{t1}) and a non-linear operation of byte addition.

Let us notice that if $\mathfrak{T} = \varphi T \varphi^{-1}$ and $\mathfrak{T}$ is the inversion of the least significant bit, then the isomorphic image of byte addition operation cannot be linear, since the equation $\varphi(\psi(x) + \psi(y)) = x + y$ is only possible with affine substitution ψ and linear substitution φ. So, let us try to make maps of diffusion substitutions M, L_t, L_{t1} affine. Supposing $M_t = L_t M$, $M_{t1} = L_{t1} M$ are affine substitutions.

Let us choose auxiliary substitutions φ, ψ, χ_1, χ_2 so that isomorphic images of bytes in the diffusion map will be only zero or identity ones (E). We get these conditions for identity substitutions:

1. $\mathfrak{T} = \varphi^{-1} T \varphi$,
2. $\mathfrak{M} = E = \psi^{-1} M \varphi$,
3. $\mathfrak{M}_t = E = {\chi_1}^{-1} M_t \varphi$,
4. $\mathfrak{M}_{t1} = E = {\chi_2}^{-1}\ M_{t1} \varphi$.

Such auxiliary substitutions ψ, χ_1, χ_2 exist and are uniquely defined.

Let us mark the AES cipher image considering the aforementioned regular automorphisms of the Zhegalkin ring of polynomials as IAES.

Theorem 5. *If* $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ *are arbitrary substitutions and* $\mathfrak{M} = \psi^{-1} M \varphi$, $\mathfrak{M}_t = {\chi_1}^{-1} M_t \varphi$, $\mathfrak{M}_{t1} = {\chi_2}^{-1} M_{t1} \varphi$, *then* φ, ψ, χ_1, χ_2 *are affinely equivalent.*

Proof The proof results from the affine equivalency definition and the fact that M, M_t, M_{t1} are affine substitutions. ■

Affine equivalency permutes probabilities of differentials, i.e. values of probabilities remain, but the type of differentials changes.

Theorem 6. *Maps* $\mathfrak{T} = \varphi^{-1} T \varphi$, $\mathfrak{M} = \psi^{-1} M \varphi$, $\mathfrak{M}_t = {\chi_1}^{-1} M_t \varphi$, $\mathfrak{M}_{t1} = {\chi_2}^{-1}\ M_{t1} \varphi$ *define the isomorphism of ciphers AES* $\to$ *IAES.*

Proof Let us see the first byte of a text after one encryption cycle in AES and IAES. Let us mark $x_1, \ldots, x_{16}$ the bytes of the input text. Transformation of the byte in AES has the following form:

$$x_1 \leftarrow (k_1 + M_t T(x_1) + M_{t1} T(x_6) + MT(x_{11}) + MT(x_{16})).$$

In IAES the initial map $(\mathbf{x})_i \leftarrow \varphi^{-1}(x_i)$, $\mathbf{k}_i \leftarrow \varphi^{-1}(k_i)$ is done. Transformation of the same byte in IAES has this form $\mathbf{x}_1 \leftarrow \phi^{-1}(\phi(\mathbf{k}_1) + \chi_1(\mathfrak{M}_t(\mathfrak{T}(\mathbf{x}_1))) + \chi_2(\mathfrak{M}_{t1}(\mathfrak{T}(\mathbf{x}_6))) + \psi(\mathfrak{M}(\mathfrak{T}(\mathbf{x_{11}}))) + \psi(\mathfrak{M}(\mathfrak{T}(\mathbf{x}_{16}))))$. Then the first summand is $\varphi(\mathbf{k}_1) = \varphi\varphi^{-1}(k_1) = k_1$. The second summand of the bracketed expression for IAES equals $\chi_1(\mathfrak{M}_t(\mathfrak{T}(\mathbf{x}_1))) = \chi_1 {\chi_1}^{-1} M_t \phi\phi^{-1} T \phi(\mathbf{x}_1) = M_t T(x_1)$ that coincides with the second summand for AES. Similarly, the third, fourth, and fifth summands for IAES coincide with the

corresponding summands for AES. The same is true for other sums of bytes. ■

So, in IAES the substitution image is an inversion of the least significant bit (with error rate 2^{-7}), map images M, M_t, M_{t1} are affine and have probability differentials 1 and linear sums with absolute dominance 0.5. Thus, in IAES there is only one non-linear operation – isomorphic image of XOR (IXOR) operation, mapping 5 bytes into one byte. This operation is obviously not a substitution, but is defined by an ideal from 48 variables (40 bits of input variables and 8 bits of output variables) and, consequently, has differentials with corresponding probabilities.

Let us examine differential and linear properties of IAES.

5. Results of the experiment and security of AES

Substitutions M, M_t, M_{t1}, φ, ψ, χ_1, χ_2 and tables of maximum dominances and linear sums are given in the appendix A.

Herein the image of XOR 5 bytes is examined as substitutions of types $\varphi^{-1}(\psi(x) + y)$, $\varphi^{-1}(\chi_1(x) + y)$, $\varphi^{-1}(\chi_2(x) + y)$ for all sorts of y. Thus, the sum of all summands, apart from one, is considered fixed. Each y defines its substitution as input function x.

In IAES cipher probabilities of differentials and dominances of linear sums of the IXOR map are defined by a boundless table. That is why the appendix includes maximum values of differential values for each of 256 y and both maximum and minimum values of dominances.

Original AES has maximum probabilities of differentials 4/256. IAES cipher per one byte of IXOR has maximum probabilities of differentials 256/256, 96/256/, 92/256. The average value of maximum probabilities by all $y = 0, \ldots, 255$ equals $34.7/256 = 0.136$. It is noticeable that maximum probabilities of differentials are on average 8.7 times higher. IAES пїSipher has absolute maximum dominances of linear sums 128/256, 72/256 for all the mentioned substitutions. It is clear that maximum dominances of linear sums are on average 3 times higher by all y in comparison with the original AES.

Let us assess the probability of differential characteristic of 10-cycle IAES accordingly [12]. In differential cryptanalysis, probabilities of differentials of non-linear dominances belonging to differential / linear characteristics are multiplied together. In each cycle, beginning from the third one, all 16 non-linear blocks participate in transformation. If in the original AES the differential probability is $2^{-6*16*7} = 2^{-672}$, then in IAES (supposing probabilities are 8 times higher from 2^{-6} to 2^{-3} on average, i.e. probability p is substituted with $\sqrt{p}$) the differential probability will be $2^{-3*16*7} = 2^{-336}$. We obtain that security of IAES (and, as a result, security of AES) is 2 times lower by the order of magnitude comparing to previous assessments. If there are 16 active non-linearities in the differential characteristic of one IAES round, complexity of a differential attack per one round decreases by $2^{3*16} = 2^{48}$ times in comparison with AES. Let us remark that when carrying out cryptanalysis of differential probabilities, dominances of linear sums can be significantly increased due to parallel branches in the characteristic. In the linear cryptanalysis, dominances for separate non-linear maps included in the linear sum get multiplied together. At this, complexity of an attack is inversely proportional to the squared dominance.

The introduced estimation is very rough. Real differential IAES cryptanalysis requires clarifying in comparison with [12], since probabilities of differentials depend on the key.

The following theorem shows that there is a mechanism that allows, on the one hand, obtaining differentials of probability 1 for IXOR and, on the other hand, inhibits propagation of active non-linearities in the differential IAES characteristic.

Theorem 7. *Let a, b, c, d be four bytes*

predetermining the following sum:

$$\varphi^{-1}(\psi(a) + \psi(b) + \chi_1(c) + \chi_2(d)).$$

Then a pair of four bytes (a, a, c, d), (a + Δ, a + Δ, c, d) gives a zero difference at the output for any Δ.

Proof Let us remark that equations $\varphi^{-1}(x) = \varphi^{-1}(y)$ and $x = y$ are carried out simultaneously. That is why operation φ^{-1}can be omitted from the condition of the theorem. Let us examine two fours of bytes $(a,\ b,\ c,\ d)$ and $(a_1,\ b_1,\ c_1,\ d_1)$, which define sums $z = \psi(a) + \psi(b) + \chi_1(c) + \chi_2(d)$ and $z_1 = \psi(a_1) + \psi(b_1) + \chi_1(c_1) + \chi_2(d_1)$. Then the equations $a = b,\ a_1 = b_1,\ c_1 = c,\ d_1 = d$ define the relation $z = z_1$. It means that a pair of four bytes $(a,\ a,\ c,\ d)$ and $(a + \Delta,\ a + \Delta,\ c,\ d)$ determines the input difference of IXOR operation, where the output difference equals 0 at any $a,\ c,\ d,\ \Delta$. Thus, a collection of these differentials has probability 1. The fact that the output probability equals 0, inhibits distribution of active non-linearities in the differential characteristic of IAES cipher. ■

Theorem 7 defines the mechanism which allows diminishing the number of active non-linearities in the differential characteristic. Let us remark that the diffusion map in AES, IAES is a substitution, acting on 16-byte words. Since no substitution can have a zero output difference at a non-zero input difference, then for each IAES round and a non-zero input difference, the output difference per all the block will also be non-zero.

As in IAES the dominance increases considerably (more than three times) and dominances for non-linearities, belonging to the linear sum, get multiplied together, the dominance of the linear sum of output in IAES per one round at 16 active non-linearities is $6{\cdot}10^7$ times more than an analogous dominance in AES. At this, the complexity of a linear attack per one round is $3.6{\cdot}10^{15}$ times lower in comparison with AES (without considering parallel branches).

The analogue of theorem 7 is, obviously, true for the linear cryptanalysis as well. So, the virtual isomorphism method gives two mechanisms to decrease security: increased probabilities of differentials (linear sums) and decreased number of active non-linearities (their number is proportional to security logarithm). This paper examines only the first mechanism.

This makes us doubt that security of IAES (and, respectively, that of AES) to the differential or linear analysis equals complexity of search for the keys.

In the research, affine substitution $\mathfrak{T}$ was used, which is only approximately conjugated with the inversion in field $\mathbb{F}_{256}$ (error rate is 2^{-7}). This error can be eliminated if substitution $\mathfrak{T}$ is changed for a quasi-affine one, where the least significant bit is defined by the polynomial $y_8 + x_8 + (1 + x_1)\ \ldots\ (1 + x_7)$. Non-linear differential probabilities of substitution $\mathfrak{T}$, in this case, equal 1 or 252/256, but maximum dominances of linear sums remain 128/256. At this, the type of substitutions φ, ψ, χ_1, χ_2 does not change.

6. Conclusions

1. The virtual isomorphism method is a prospective tool of cryptanalysis. It allows us to change an approach to analysis of ciphers. A cryptanalyst, when examining a cipher, used to search for a new cryptanalysis method for which the cipher was vulnerable (while ciphers are designed to withstand the known attacks). Today a cryptanalyst that has the knowledge of some universal cryptanalysis method and examines a cipher, can just choose a suitable isomorphism the isomorphic cipher will be vulnerable to for the chosen cryptanalysis method.

2. Apparently, the strength of AES to differential and linear cryptanalysis is considerably lower than it is commonly believed.

3. These findings can be extended on AES-like ciphers, where the diffusion map

forces on the same length words as a substitution. For these ciphers there is a class of supposedly weak substitutions. A substitution is supposedly weak if it is affinely equivalent to the substitution of the same or almost the same cycle type as a specific affine substitution. Evidently, this class of substitutions is very vast. It is not known if there are substitutions which are not supposedly weak. An algorithm to recognize supposedly weak substitutions is not known.

4. Strength of an AES-like cipher with a supposedly weak substitution is determined by the virtual isomorphism in use, rather than by properties of the substitution itself. That is why it can be expected that the choice of special substitutions does not allow increasing the strength of the cipher considerably in comparison with arbitrary substitutions (it may be assumed that it is impossible to recognize a supposedly weak substitution).

Appendix A: Auxiliary maps, differentials and linear sums of IAES cipher

Substitution orbits Orb(x, $\langle T,\mathcal{T} \rangle$) equal to
Orb = {{0, 1}, {2, 3, 246, 247, 140, 141}, {4, 5, 82, 83, 202, 203}, {6, 7, 209, 208, 122, 123}, {8, 9, 79, 78, 233, 232}, {10, 11, 192, 193, 40, 41}, {12, 13, 225, 224, 177, 176}, {14, 15, 199, 198, 228, 229}, {16, 17, 180, 181, 117, 116}, {18, 19, 75, 74, 171, 170}, {20, 21, 43, 42, 152, 153}, {22, 23, 95, 94, 97, 96}, {24, 25, 63, 62, 89, 88}, {26, 27, 204, 205, 252, 253}, {28, 29, 64, 65, 254, 255}, {30, 31, 178, 179, 239, 238}, {32, 33, 110, 111, 59, 58}, {34, 35, 241, 240, 91, 90}, {36, 37, 77, 76, 84, 85}, {38, 39, 201, 200, 169, 168}, {44, 45, 68, 69, 49, 48}, {46, 47, 194, 195, 163, 162}, {50, 51, 108, 109, 147, 146}, {52, 53, 57, 56, 242, 243}, {54, 55, 66, 67, 103, 102}, {60, 61, 187, 186, 118, 119}, {70, 71, 105, 104, 244, 245}, {72, 73, 100, 101, 166, 167}, {80, 81, 92, 93, 236, 237}, {86, 87, 191, 190, 134, 135}, {98, 99, 211, 210, 174, 175}, {106, 107, 223, 222, 144, 145}, {112, 113, 183, 182, 120, 121}, {114, 115, 133, 132, 150, 151}, {124, 125, 250, 251, 160, 161}, {126, 127, 130, 131, 128, 129}, {136, 137, 158, 159, 154, 155}, {138, 139, 217, 216, 148, 149}, {142, 143, 164, 165, 184, 185}, {156, 157, 220, 221, 248, 249}, {172, 173, 231, 230, 207, 206}, {188, 189}, {196, 197, 212, 213, 219, 218}, {214, 215, 234, 235, 227, 226}}.

Substitutions M, M_t, M_{t1} equal respectively to
M = {99, 124, 93, 66, 31, 0, 33, 62, 155, 132, 165, 186, 231, 248, 217, 198, 146, 141, 172, 179, 238, 241, 208, 207, 106, 117, 84, 75, 22, 9, 40, 55, 128, 159, 190, 161, 252, 227, 194, 221, 120, 103, 70, 89, 4, 27, 58, 37, 113, 110, 79, 80, 13, 18, 51, 44, 137, 150, 183, 168, 245, 234, 203, 212, 164, 187, 154, 133, 216, 199, 230, 249, 92, 67, 98, 125, 32, 63, 30, 1, 85, 74, 107, 116, 41, 54, 23, 8, 173, 178, 147, 140, 209, 206, 239, 240, 71, 88, 121, 102, 59, 36, 5, 26, 191, 160, 129, 158, 195, 220, 253, 226, 182, 169, 136, 151, 202, 213, 244, 235, 78, 81, 112, 111, 50, 45, 12, 19, 236, 243, 210, 205, 144, 143, 174, 177, 20, 11, 42, 53, 104, 119, 86, 73, 29, 2, 35, 60, 97, 126, 95, 64, 229, 250, 219, 196, 153, 134, 167, 184, 15, 16, 49, 46, 115, 108, 77, 82, 247, 232, 201, 214, 139, 148, 181, 170, 254, 225, 192, 223, 130, 157, 188, 163, 6, 25, 56, 39, 122, 101, 68, 91, 43, 52, 21, 10, 87, 72, 105, 118, 211, 204, 237, 242, 175, 176, 145, 142, 218, 197, 228, 251, 166, 185, 152, 135, 34, 61, 28, 3, 94, 65, 96, 127, 200, 215, 246, 233, 180, 171, 138, 149, 48, 47, 14, 17, 76, 83, 114, 109, 57, 38, 7, 24, 69, 90, 123, 100, 193, 222, 255, 224, 189, 162, 131, 156};
M_t = {177, 62, 46, 161, 143, 0, 16, 159, 205, 66, 82, 221, 243, 124, 108, 227, 73, 198, 214, 89, 119, 248, 232, 103, 53, 186, 170, 37, 11, 132, 148, 27, 64, 207, 223, 80, 126, 241, 225, 110, 60, 179, 163, 44, 2, 141, 157, 18, 184, 55, 39, 168, 134, 9, 25, 150, 196, 75, 91, 212, 250, 117, 101, 234, 210, 93, 77, 194, 236, 99, 115, 252, 174, 33, 49, 190, 144, 31, 15, 128, 42, 165, 181, 58, 20, 155, 139, 4, 86, 217, 201, 70, 104, 231, 247, 120, 35, 172, 188, 51, 29, 146, 130, 13, 95, 208, 192, 79, 97, 238, 254,

113, 219, 84, 68, 203, 229, 106, 122, 245, 167, 40, 56, 183, 153, 22, 6, 137, 246, 121, 105, 230, 200, 71, 87, 216, 138, 5, 21, 154, 180, 59, 43, 164, 14, 129, 145, 30, 48, 191, 175, 32, 114, 253, 237, 98, 76, 195, 211, 92, 7, 136, 152, 23, 57, 182, 166, 41, 123, 244, 228, 107, 69, 202, 218, 85, 255, 112, 96, 239, 193, 78, 94, 209, 131, 12, 28, 147, 189, 50, 34, 173, 149, 26, 10, 133, 171, 36, 52, 187, 233, 102, 118, 249, 215, 88, 72, 199, 109, 226, 242, 125, 83, 220, 204, 67, 17, 158, 142, 1, 47, 160, 176, 63, 100, 235, 251, 116, 90, 213, 197, 74, 24, 151, 135, 8, 38, 169, 185, 54, 156, 19, 3, 140, 162, 45, 61, 178, 224, 111, 127, 240, 222, 81, 65, 206};

M_{t1} = {210, 66, 115, 227, 144, 0, 49, 161, 86, 198, 247, 103, 20, 132, 181, 37, 219, 75, 122, 234, 153, 9, 56, 168, 95, 207, 254, 110, 29, 141, 188, 44, 192, 80, 97, 241, 130, 18, 35, 179, 68, 212, 229, 117, 6, 150, 167, 55, 201, 89, 104, 248, 139, 27, 42, 186, 77, 221, 236, 124, 15, 159, 174, 62, 118, 230, 215, 71, 52, 164, 149, 5, 242, 98, 83, 195, 176, 32, 17, 129, 127, 239, 222, 78, 61, 173, 156, 12, 251, 107, 90, 202, 185, 41, 24, 136, 100, 244, 197, 85, 38, 182, 135, 23, 224, 112, 65, 209, 162, 50, 3, 147, 109, 253, 204, 92, 47, 191, 142, 30, 233, 121, 72, 216, 171, 59, 10, 154, 26, 138, 187, 43, 88, 200, 249, 105, 158, 14, 63, 175, 220, 76, 125, 237, 19, 131, 178, 34, 81, 193, 240, 96, 151, 7, 54, 166, 213, 69, 116, 228, 8, 152, 169, 57, 74, 218, 235, 123, 140, 28, 45, 189, 206, 94, 111, 255, 1, 145, 160, 48, 67, 211, 226, 114, 133, 21, 36, 180, 199, 87, 102, 246, 190, 46, 31, 143, 252, 108, 93, 205, 58, 170, 155, 11, 120, 232, 217, 73, 183, 39, 22, 134, 245, 101, 84, 196, 51, 163, 146, 2, 113, 225, 208, 64, 172, 60, 13, 157, 238, 126, 79, 223, 40, 184, 137, 25, 106, 250, 203, 91, 165, 53, 4, 148, 231, 119, 70, 214, 33, 177, 128, 16, 99, 243, 194, 82}.

Auxiliary substitutions equal to

ϕ = {0, 1, 246, 3, 82, 5, 209, 7, 79, 9, 192, 11, 225, 13, 199, 15, 180, 17, 75, 19, 43, 21, 95, 23, 63, 25, 204, 27, 64, 29, 178, 31, 110, 33, 241, 35, 77, 37, 201, 39, 10, 41, 42, 152, 68, 45, 194, 47, 48, 44, 108, 51, 57, 53, 66, 55, 56, 242, 58, 32, 187, 61, 62, 89, 254, 65, 103, 67, 49, 69, 105, 71, 100, 73, 74, 171, 76, 84, 78, 233, 92, 81, 202, 83, 36, 85, 191, 87, 88, 24, 90, 34, 236, 93, 94, 97, 96, 22, 211, 99, 166, 101, 102, 54, 104, 244, 223, 107, 147, 109, 59, 111, 183, 113, 133, 115, 116, 16, 60, 119, 112, 121, 6, 123, 250, 125, 130, 127, 126, 129, 128, 131, 132, 150, 86, 135, 158, 137, 217, 139, 2, 141, 164, 143, 106, 145, 146, 50, 138, 149, 114, 151, 20, 153, 136, 155, 220, 157, 154, 159, 124, 161, 162, 46, 184, 165, 72, 167, 168, 38, 170, 18, 231, 173, 98, 175, 176, 12, 239, 179, 117, 181, 182, 120, 142, 185, 186, 118, 188, 189, 190, 134, 40, 193, 163, 195, 212, 197, 198, 228, 200, 169, 4, 203, 252, 205, 206, 172, 208, 122, 210, 174, 219, 213, 234, 215, 216, 148, 218, 196, 248, 221, 222, 144, 224, 177, 226, 214, 14, 229, 230, 207, 232, 8, 227, 235, 80, 237, 238, 30, 240, 91, 52, 243, 70, 245, 140, 247, 156, 249, 160, 251, 26, 253, 28, 255};

ψ = {99, 124, 123, 66, 107, 0, 197, 62, 1, 132, 43, 186, 215, 248, 118, 198, 130, 141, 125, 179, 89, 241, 240, 207, 212, 117, 175, 75, 164, 9, 192, 55, 253, 159, 38, 161, 63, 227, 204, 221, 165, 103, 70, 229, 216, 27, 21, 37, 113, 4, 195, 80, 150, 18, 154, 44, 137, 7, 183, 128, 39, 234, 203, 178, 131, 187, 26, 133, 110, 199, 160, 249, 59, 67, 98, 214, 32, 41, 30, 47, 209, 74, 237, 116, 252, 54, 91, 8, 173, 106, 147, 190, 76, 206, 239, 88, 71, 208, 251, 102, 77, 36, 5, 51, 191, 69, 127, 158, 60, 220, 168, 226, 163, 169, 143, 151, 202, 146, 245, 235, 182, 81, 33, 111, 255, 45, 210, 19, 12, 243, 236, 205, 144, 95, 23, 177, 167, 11, 61, 53, 93, 119, 115, 73, 129, 2, 35, 79, 42, 126, 136, 64, 238, 250, 20, 196, 94, 134, 219, 184, 50, 16, 49, 58, 6, 108, 92, 82, 247, 194, 201, 172, 149, 148, 121, 170, 254, 231, 109, 223, 213, 157, 188, 78, 86, 25, 56, 244, 122, 101, 68, 174, 120, 52, 46, 10, 166, 72, 105, 180, 211, 232, 31, 242, 189, 176, 145, 139, 218, 112, 228, 181, 3, 185, 14, 135, 34, 97, 28, 87, 193, 65, 96, 29, 200, 225, 246, 152, 217, 171, 138, 142, 48, 155, 233, 17, 85, 83, 114, 40, 57, 140, 13, 24, 230, 90, 104, 100, 153, 222, 15, 224, 84, 162, 22, 156};

χ_1 = {177, 62, 61, 161, 181, 0, 226, 159, 128, 66, 149, 221, 235, 124, 187, 227, 193, 198, 190, 89, 44, 248, 120, 103, 234, 186, 215, 37, 210, 132, 96, 27, 254, 207, 19, 80, 31, 241, 102, 110, 82, 179, 163, 114, 236, 141, 10, 18, 184, 2, 97, 168, 75, 9, 77, 150, 196, 3, 91, 64, 147, 117, 101, 217, 65, 93, 13, 194, 55, 99, 208, 252, 29, 33, 49, 107, 144, 20, 15, 151, 104, 165, 118, 58, 126, 155, 173, 4, 86, 53, 201, 223, 38, 231, 247, 172, 35, 232, 125, 51, 166,

146, 130, 25, 95, 162, 63, 79, 30, 238, 212, 113, 209, 84, 71, 203, 229, 73, 250, 245, 219, 40, 16, 183, 127, 22, 105, 137, 6, 121, 246, 230, 200, 175, 139, 216, 211, 5, 158, 154, 46, 59, 57, 164, 192, 129, 145, 39, 21, 191, 68, 32, 119, 253, 138, 98, 47, 195, 237, 92, 153, 136, 152, 157, 131, 182, 174, 41, 123, 225, 228, 214, 74, 202, 188, 85, 255, 243, 54, 239, 106, 78, 94, 167, 43, 12, 28, 122, 189, 50, 34, 87, 60, 26, 23, 133, 83, 36, 52, 90, 233, 244, 143, 249, 222, 88, 72, 69, 109, 56, 242, 218, 1, 220, 135, 67, 17, 48, 142, 171, 224, 160, 176, 14, 100, 112, 251, 204, 108, 213, 197, 199, 24, 205, 116, 8, 42, 169, 185, 148, 156, 70, 134, 140, 115, 45, 180, 178, 76, 111, 7, 240, 170, 81, 11, 206};

χ_2 = {210, 66, 70, 227, 222, 0, 39, 161, 129, 198, 190, 103, 60, 132, 205, 37, 67, 75, 195, 234, 117, 9, 136, 168, 62, 207, 120, 110, 118, 141, 160, 44, 3, 80, 53, 241, 32, 18, 170, 179, 247, 212, 229, 151, 52, 150, 31, 55, 201, 6, 162, 248, 221, 27, 215, 186, 77, 4, 236, 192, 180, 159, 174, 107, 194, 230, 23, 71, 89, 164, 112, 5, 38, 98, 83, 189, 176, 61, 17, 184, 185, 239, 155, 78, 130, 173, 246, 12, 251, 95, 90, 97, 106, 41, 24, 244, 100, 56, 134, 85, 235, 182, 135, 42, 224, 231, 64, 209, 34, 50, 124, 147, 114, 253, 200, 92, 47, 219, 15, 30, 109, 121, 49, 216, 128, 59, 187, 154, 10, 138, 26, 43, 88, 240, 156, 105, 116, 14, 163, 175, 115, 76, 74, 237, 65, 131, 178, 104, 63, 193, 204, 96, 153, 7, 158, 166, 113, 69, 54, 228, 171, 152, 169, 167, 133, 218, 242, 123, 140, 35, 45, 122, 223, 94, 197, 255, 1, 20, 91, 48, 191, 211, 226, 233, 125, 21, 36, 142, 199, 87, 102, 249, 68, 46, 57, 143, 245, 108, 93, 238, 58, 28, 144, 11, 99, 232, 217, 206, 183, 72, 22, 111, 2, 101, 137, 196, 51, 81, 146, 252, 33, 225, 208, 19, 172, 145, 13, 84, 181, 126, 79, 73, 40, 86, 157, 25, 127, 250, 203, 188, 165, 202, 139, 148, 149, 119, 220, 214, 213, 177, 8, 16, 254, 243, 29, 82}.

Differentials and linear sums of the IXOR map in IAES cipher are defined by a boundless table. To study the properties of this table let us examine the sections of this map by each byte, i.e. byte substitution of type $\varphi^{-1}(\varphi(x) + y)$, $\varphi^{-1}(\psi(x) + y)$, $\varphi^{-1}(\chi_1(x) + y)$, $\varphi^{-1}(\chi_2(x) + y)$. Each y defines its substitution as input function x. For each $y = 0, 1, \ldots, 255$ probabilities of the most probable differentials of the aforementioned 5 substitutions equal respectively (the table element has to be divided by 256):

{256, 6, 82, 50, 76, 56, 90, 42, 88, 44, 78, 54, 70, 70, 80, 56, 84, 52, 84, 48, 90, 42, 86, 46, 72, 64, 64, 68, 76, 60, 70, 66, 68, 64, 68, 72, 64, 72, 72, 60, 80, 56, 78, 58, 76, 56, 82, 50, 82, 54, 72, 60, 64, 68, 76, 60, 92, 44, 82, 50, 68, 64, 86, 50, 68, 64, 72, 60, 64, 68, 60, 72, 64, 68, 86, 50, 80, 52, 66, 70, 72, 64, 70, 62, 70, 62, 76, 56, 86, 46, 76, 56, 78, 62, 88, 48, 86, 46, 82, 54, 90, 42, 84, 48, 70, 66, 72, 60, 74, 58, 74, 58, 92, 44, 86, 46, 92, 44, 72, 60, 76, 56, 74, 58, 72, 68, 64, 68, 96, 36, 82, 50, 88, 44, 86, 46, 88, 44, 76, 56, 70, 66, 80, 52, 84, 48, 82, 50, 80, 52, 82, 50, 72, 60, 72, 60, 76, 56, 64, 68, 64, 72, 66, 66, 64, 68, 68, 64, 78, 54, 74, 62, 76, 60, 84, 48, 74, 66, 68, 68, 64, 72, 70, 62, 80, 52, 82, 50, 82, 56, 82, 54, 60, 72, 68, 64, 64, 68, 58, 78, 76, 60, 84, 56, 68, 68, 70, 62, 78, 58, 66, 66, 58, 74, 84, 56, 82, 50, 76, 56, 78, 54, 86, 46, 82, 50, 88, 48, 86, 46, 84, 52, 82, 58, 72, 64, 72, 60, 74, 58, 88, 48, 78, 54, 76, 56, 74, 58, 72, 60, 76, 60, 68, 64, 64, 72};

{30, 32, 32, 38, 32, 38, 34, 34, 30, 38, 36, 32, 28, 36, 28, 32, 32, 40, 32, 34, 34, 32, 26, 40, 36, 32, 30, 36, 34, 32, 30, 40, 34, 38, 36, 32, 32, 38, 40, 32, 28, 38, 32, 34, 36, 38, 34, 34, 36, 36, 34, 32, 36, 32, 32, 42, 32, 34, 32, 34, 34, 38, 34, 36, 32, 36, 32, 36, 42, 34, 38, 38, 30, 38, 36, 36, 32, 40, 28, 38, 34, 40, 38, 34, 34, 36, 32, 32, 28, 42, 32, 32, 32, 36, 32, 34, 32, 34, 30, 40, 38, 36, 32, 42, 32, 38, 30, 30, 34, 32, 28, 42, 28, 36, 36, 38, 36, 36, 36, 34, 28, 38, 32, 38, 32, 38, 34, 32, 30, 36, 34, 32, 36, 34, 28, 36, 38, 34, 34, 34, 34, 40, 36, 34, 32, 34, 38, 34, 34, 30, 30, 36, 32, 38, 38, 28, 40, 32, 38, 42, 34, 38, 36, 38, 34, 34, 32, 36, 32, 36, 36, 32, 36, 36, 38, 38, 36, 36, 34, 34, 38, 32, 38, 42, 34, 36, 38, 30, 34, 32, 32, 34, 32, 36, 30, 34, 38, 30, 36, 40, 32, 38, 34, 38, 30, 36, 34, 34, 34, 32, 32, 36, 34, 38, 36, 34, 34, 32, 34, 32, 36, 38, 34, 34, 36, 34, 30, 36, 32, 30, 30, 36, 36, 36, 30, 40, 36, 32, 36, 36, 34, 32, 34, 34, 34, 36, 32, 38, 34, 38, 38, 36, 34, 34, 34, 34};

{34, 34, 38, 34, 34, 36, 38, 34, 40, 34, 32, 36, 30, 34, 32, 40, 34, 34, 28, 34, 34, 36, 36, 38, 32, 40, 36, 36, 36, 40, 32, 34, 36, 36, 38, 32, 34, 34, 42,

32, 40, 32, 30, 42, 34, 30, 34, 38, 36, 34, 32, 32, 36, 36, 34, 34, 36, 40, 32, 38, 32, 38, 32, 30, 32, 38, 36, 34, 38, 38, 32, 34, 36, 40, 32, 34, 38, 32, 32, 34, 36, 34, 34, 34, 38, 30, 34, 34, 30, 34, 36, 32, 34, 34, 36, 36, 34, 32, 36, 30, 38, 36, 36, 34, 38, 32, 34, 30, 36, 32, 34, 38, 38, 34, 44, 36, 36, 26, 38, 34, 34, 32, 38, 30, 38, 32, 36, 34, 32, 34, 38, 34, 32, 36, 36, 38, 36, 32, 30, 36, 32, 32, 32, 40, 34, 34, 30, 36, 36, 36, 32, 34, 36, 42, 34, 36, 34, 42, 34, 34, 30, 34, 38, 34, 34, 34, 42, 30, 36, 34, 30, 40, 38, 30, 34, 36, 36, 34, 32, 34, 34, 36, 32, 34, 38, 38, 36, 36, 36, 38, 32, 32, 34, 38, 36, 32, 38, 38, 34, 30, 36, 38, 34, 36, 38, 32, 36, 34, 32, 34, 34, 34, 42, 28, 34, 32, 34, 34, 38, 32, 36, 34, 36, 36, 34, 34, 36, 32, 40, 36, 38, 30, 38, 34, 32, 32, 36, 32, 32, 34, 40, 36, 44, 32, 38, 32, 36, 32, 34, 30, 38, 30, 36, 32, 36, 34};

{30, 28, 30, 34, 40, 28, 36, 32, 38, 34, 46, 28, 32, 34, 32, 40, 30, 46, 34, 36, 36, 38, 38, 36, 34, 36, 30, 44, 32, 36, 30, 40, 30, 40, 32, 34, 36, 38, 34, 36, 38, 30, 36, 30, 34, 38, 34, 38, 32, 36, 34, 36, 36, 28, 34, 30, 38, 32, 36, 34, 32, 36, 32, 32, 32, 34, 32, 38, 36, 36, 34, 34, 36, 38, 30, 32, 32, 36, 30, 36, 34, 36, 36, 34, 40, 32, 34, 36, 40, 34, 44, 34, 38, 36, 40, 36, 32, 38, 34, 34, 36, 34, 36, 32, 42, 36, 34, 32, 32, 38, 30, 38, 28, 34, 34, 36, 34, 36, 34, 34, 34, 36, 36, 34, 28, 38, 30, 36, 36, 28, 38, 34, 40, 34, 30, 36, 30, 34, 38, 32, 40, 32, 36, 32, 36, 38, 36, 38, 26, 44, 32, 36, 30, 36, 32, 38, 34, 38, 34, 42, 36, 36, 34, 34, 32, 34, 28, 36, 36, 38, 34, 40, 38, 38, 36, 36, 40, 32, 34, 30, 34, 36, 32, 36, 38, 36, 34, 30, 36, 28, 36, 32, 30, 38, 36, 34, 32, 36, 30, 36, 32, 34, 30, 38, 34, 36, 34, 34, 36, 36, 34, 38, 30, 34, 34, 32, 36, 38, 40, 34, 42, 30, 44, 32, 36, 30, 34, 30, 32, 38, 32, 34, 34, 36, 32, 38, 32, 38, 36, 38, 40, 34, 36, 36, 34, 38, 30, 36, 32, 36, 30, 36, 36, 32, 36, 32};

Maximum and minimum dominances of linear sums of the aforementioned substitutions for each $y = 0, \ldots, 255$ equal respectively (table values have to be divided by 256):

{128, 16, 68, 48, 60, 52, 68, 48, 60, 44, 60, 48, 52, 60, 68, 48, 64, 44, 64, 44, 64, 44, 68, 40, 56, 52, 56, 56, 56, 52, 56, 52, 56, 60, 52, 52, 56, 56, 60, 52, 56, 52, 56, 52, 68, 48, 60, 44, 60, 48, 56, 52, 56, 56, 52, 52, 64, 40, 68, 48, 60, 56, 68, 44, 60, 56, 56, 44, 52, 56, 52, 56, 56, 64, 64, 40, 64, 48, 60, 60, 56, 48, 56, 56, 56, 52, 56, 56, 68, 40, 60, 48, 60, 52, 60, 52, 64, 44, 60, 48, 68, 40, 72, 44, 60, 52, 64, 52, 60, 44, 60, 48, 64, 40, 64, 48, 64, 40, 60, 52, 60, 52, 60, 52, 52, 48, 56, 56, 68, 40, 60, 52, 60, 44, 60, 44, 68, 44, 56, 52, 52, 52, 64, 44, 60, 44, 60, 48, 60, 52, 60, 44, 60, 52, 56, 48, 60, 48, 60, 56, 48, 60, 52, 56, 52, 52, 56, 52, 64, 52, 56, 48, 60, 52, 68, 40, 56, 48, 52, 56, 68, 52, 56, 56, 60, 40, 64, 40, 60, 48, 64, 48, 52, 60, 52, 56, 56, 56, 48, 60, 56, 52, 64, 52, 52, 52, 56, 52, 56, 48, 60, 52, 52, 60, 68, 44, 64, 56, 60, 48, 64, 48, 60, 40, 68, 48, 60, 44, 64, 52, 68, 48, 60, 44, 56, 52, 56, 52, 64, 48, 68, 52, 60, 44, 60, 48, 60, 48, 56, 52, 64, 56, 60, 56, 56, 56};

{-128, -16, -60, -44, -56, -30, -64, -40, -60, -42, -60, -52, -56, -52, -60, -44, -64, -44, -64, -40, -68, -40, -60, -48, -56, -48, -52, -60, -64, -48, -56, -56, -64, -56, -52, -56, -60, -56, -56, -60, -56, -44, -64, -52, -60, -48, -68, -48, -56, -48, -60, -48, -56, -56, -60, -52, -68, -40, -56, -56, -52, -48, -60, -44, -60, -52, -56, -52, -52, -52, -52, -52, -56, -52, -64, -48, -64, -48, -52, -56, -52, -52, -56, -52, -56, -48, -68, -52, -64, -44, -60, -44, -60, -56, -72, -48, -60, -44, -64, -52, -64, -48, -68, -40, -64, -52, -56, -56, -56, -52, -60, -48, -68, -40, -64, -44, -68, -44, -56, -52, -60, -48, -56, -52, -56, -56, -52, -56, -64, -36, -68, -52, -68, -40, -60, -44, -68, -40, -60, -44, -52, -56, -60, -52, -60, -44, -64, -48, -60, -52, -68, -48, -52, -52, -60, -52, -56, -52, -56, -52, -56, -56, -52, -52, -52, -60, -52, -52, -60, -48, -56, -48, -64, -60, -68, -44, -64, -56, -56, -52, -60, -60, -56, -52, -60, -48, -60, -48, -60, -52, -64, -48, -52, -60, -52, -52, -56, -56, -52, -64, -60, -48, -68, -52, -48, -56, -60, -52, -56, -60, -52, -56, -52, -56, -60, -52, -60, -48, -60, -44, -56, -48, -72, -52, -64, -52, -64, -44, -64, -44, -60, -48, -56, -52, -52, -52, -56, -52, -60, -48, -64, -40, -60, -44, -56, -48, -64, -60, -56, -48, -56, -52, -52, -56, -60, -56};

{54, 48, 46, 58, 50, 48, 50, 48, 46, 52, 54, 46, 48, 48, 52, 48, 54, 52, 48, 56, 52, 44, 48, 50, 52, 48, 48, 48, 48, 46, 46, 50, 48, 52, 46, 52, 46, 52, 50, 48, 48, 52, 48, 48, 48, 50, 44, 50, 52, 48, 46, 48, 54, 50, 46, 50, 50, 44, 48, 52, 46, 46, 50, 52, 46, 52, 46, 52, 54, 48, 48, 52, 44, 54, 56, 50, 50, 42, 44, 52, 42, 46, 48, 48, 50, 52, 50, 52, 46, 50, 46,

48, 44, 52, 46, 52, 46, 48, 48, 56, 46, 52, 52, 50, 44, 50, 52, 48, 48, 48, 44, 48, 46, 52, 50, 46, 48, 48, 52, 50, 46, 52, 46, 48, 46, 54, 48, 52, 48, 50, 54, 44, 46, 50, 50, 54, 50, 50, 52, 44, 50, 54, 48, 46, 48, 50, 52, 52, 48, 46, 50, 50, 48, 48, 54, 44, 52, 48, 50, 46, 54, 50, 48, 44, 54, 44, 46, 54, 48, 46, 46, 48, 52, 50, 50, 56, 46, 50, 44, 46, 48, 48, 48, 50, 48, 48, 50, 46, 52, 50, 48, 46, 44, 48, 58, 48, 50, 46, 50, 46, 44, 50, 50, 58, 52, 50, 52, 46, 50, 48, 48, 50, 44, 50, 52, 50, 46, 46, 52, 52, 50, 48, 46, 48, 50, 50, 46, 54, 48, 44, 52, 50, 46, 50, 44, 56, 54, 50, 48, 50, 46, 48, 50, 48, 48, 48, 48, 52, 52, 52, 50, 50, 44, 46, 50, 46};

{-46, -48, -48, -52, -46, -56, -56, -54, -48, -50, -50, -46, -46, -46, -50, -48, -50, -54, -48, -50, -52, -44, -46, -50, -46, -44, -46, -50, -46, -50, -46, -50, -48, -52, -52, -48, -48, -48, -46, -46, -46, -50, -52, -48, -50, -46, -50, -46, -48, -46, -46, -56, -50, -50, -54, -46, -52, -50, -48, -52, -46, -50, -54, -50, -44, -52, -52, -50, -50, -46, -46, -46, -48, -50, -54, -48, -50, -48, -42, -56, -46, -54, -56, -50, -44, -50, -46, -48, -54, -54, -50, -54, -46, -50, -48, -50, -48, -52, -44, -32, -48, -50, -44, -48, -46, -54, -48, -52, -50, -46, -44, -50, -46, -52, -48, -48, -50, -52, -48, -50, -48, -50, -50, -48, -44, -50, -50, -50, -48, -46, -50, -46, -46, -46, -46, -50, -54, -52, -48, -48, -46, -50, -50, -46, -46, -50, -48, -48, -48, -46, -48, -50, -48, -54, -52, -48, -52, -48, -52, -50, -52, -44, -50, -46, -50, -48, -48, -50, -48, -50, -50, -48, -50, -48, -48, -50, -50, -48, -48, -50, -54, -46, -58, -50, -44, -48, -48, -48, -52, -50, -52, -50, -54, -50, -52, -46, -50, -48, -48, -50, -48, -46, -50, -50, -46, -54, -48, -46, -48, -46, -46, -44, -48, -48, -50, -50, -48, -48, -54, -46, -50, -52, -48, -46, -48, -46, -44, -50, -52, -50, -48, -46, -54, -50, -50, -52, -46, -54, -52, -46, -48, -46, -56, -48, -54, -50, -50, -46, -50, -46, -50, -46, -48};

{54, 54, 50, 52, 44, 48, 46, 56, 52, 46, 44, 50, 44, 56, 46, 48, 50, 50, 42, 50, 44, 54, 48, 48, 46, 50, 48, 48, 46, 48, 50, 52, 52, 46, 50, 46, 46, 58, 50, 44, 52, 48, 50, 50, 48, 48, 44, 50, 48, 52, 48, 46, 46, 54, 46, 46, 48, 46, 50, 50, 46, 54, 48, 48, 52, 50, 48, 46, 50, 52, 46, 48, 48, 44, 48, 50, 48, 46, 52, 50, 48, 46, 44, 46, 52, 50, 46, 50, 46, 50, 50, 44, 50, 54, 48, 50, 50, 58, 46, 44, 48, 50, 46, 48, 48, 46, 46, 48, 48, 46, 46, 52, 48, 52, 50, 50, 52, 44, 54, 48, 52, 52, 52, 44, 50, 50, 48, 50, 46, 50, 52, 50, 48, 56, 48, 48, 48, 50, 44, 48, 56, 50, 48, 50, 50, 46, 50, 52, 42, 48, 46, 54, 48, 52, 44, 46, 46, 52, 48, 50, 46, 50, 48, 46, 48, 50, 50, 44, 54, 48, 46, 46, 54, 42, 52, 48, 50, 50, 46, 50, 46, 52, 48, 44, 52, 48, 58, 46, 48, 46, 46, 44, 50, 50, 52, 50, 50, 50, 52, 50, 46, 52, 50, 48, 50, 44, 46, 52, 46, 48, 52, 48, 48, 46, 50, 48, 48, 48, 50, 46, 52, 48, 48, 48, 48, 46, 50, 50, 54, 50, 48, 50, 52, 44, 44, 46, 52, 46, 50, 50, 50, 48, 52, 48, 48, 50, 52, 48, 52, 50, 52, 48, 54, 46, 54, 50};

{-46, -46, -46, -52, -46, -54, -46, -52, -48, -52, -48, -46, -46, -52, -48, -46, -48, -50, -46, -50, -52, -54, -46, -48, -46, -52, -48, -52, -48, -50, -48, -54, -50, -50, -52, -42, -44, -50, -48, -48, -48, -46, -42, -46, -48, -52, -46, -50, -52, -50, -50, -52, -48, -48, -46, -54, -46, -52, -46, -52, -48, -50, -52, -46, -48, -52, -48, -44, -50, -54, -48, -46, -48, -48, -46, -50, -52, -48, -48, -50, -48, -46, -46, -48, -48, -50, -50, -48, -50, -46, -50, -48, -48, -50, -50, -48, -50, -46, -52, -48, -46, -50, -48, -48, -48, -44, -52, -52, -48, -46, -42, -52, -50, -52, -56, -48, -52, -46, -54, -46, -50, -48, -50, -50, -48, -50, -54, -48, -48, -46, -46, -46, -48, -48, -46, -48, -50, -50, -46, -46, -52, -48, -48, -50, -50, -54, -50, -48, -52, -48, -46, -50, -48, -52, -50, -52, -50, -54, -50, -46, -48, -48, -44, -46, -46, -46, -56, -46, -56, -44, -48, -52, -52, -50, -44, -48, -48, -32, -46, -48, -52, -52, -48, -48, -50, -48, -50, -46, -50, -50, -52, -48, -48, -48, -50, -48, -46, -48, -52, -44, -48, -56, -46, -48, -54, -48, -44, -54, -46, -48, -48, -56, -46, -46, -48, -50, -48, -56, -52, -44, -50, -50, -52, -52, -46, -46, -52, -46, -50, -50, -52, -46, -48, -44, -48, -52, -56, -48, -48, -50, -52, -44, -48, -48, -50, -54, -50, -46, -50, -46, -48, -42, -52, -46, -46, -52};

{48, 46, 48, 46, 50, 44, 52, 52, 48, 46, 54, 46, 48, 50, 52, 50, 46, 48, 46, 48, 52, 52, 52, 44, 54, 48, 46, 56, 46, 56, 44, 56, 42, 50, 44, 52, 46, 50, 48, 46, 52, 46, 48, 48, 48, 48, 48, 50, 46, 48, 44, 46, 58, 50, 50, 50, 46, 44, 52, 44, 50, 48, 48, 44, 48, 50, 46, 50, 48, 48, 48, 46, 48, 44, 48, 52, 48, 48, 54, 56, 50, 50, 50, 46, 50, 46, 52, 48, 48, 48, 46, 44, 50, 44, 50, 46, 42, 50, 50, 54, 50, 50, 50, 46, 54, 52, 48, 46, 48, 52, 50, 48, 48, 48, 48, 46, 50, 46, 52, 46, 48, 48, 54, 44, 44, 48, 48, 48, 52, 48, 50, 48, 50, 46, 42, 54, 50, 50, 50, 46, 52, 48, 52,

50, 50, 50, 50, 52, 44, 50, 52, 50, 56, 52, 44, 52, 48, 46, 48, 48, 46, 48, 48, 46, 48, 52, 52, 44, 46, 50, 50, 50, 50, 54, 48, 50, 50, 44, 48, 46, 48, 48, 46, 52, 46, 50, 48, 52, 48, 44, 50, 46, 44, 54, 50, 48, 54, 50, 48, 44, 48, 54, 46, 56, 44, 52, 48, 52, 50, 44, 50, 46, 52, 52, 52, 48, 52, 48, 50, 54, 50, 46, 58, 50, 50, 46, 48, 48, 54, 52, 48, 48, 50, 48, 50, 50, 46, 50, 50, 50, 52, 48, 48, 48, 48, 48, 46, 52, 46, 46, 46, 48, 54, 48, 50, 46};

{-50, -46, -48, -48, -54, -46, -48, -48, -48, -42, -56, -42, -54, -50, -48, -48, -48, -50, -50, -50, -46, -46, -52, -48, -46, -48, -48, -62, -48, -52, -44, -48, -44, -56, -50, -54, -50, -48, -48, -48, -50, -46, -50, -50, -48, -48, -48, -52, -44, -50, -52, -48, -52, -46, -50, -50, -50, -50, -50, -46, -48, -52, -46, -48, -48, -50, -46, -52, -48, -44, -50, -50, -52, -52, -48, -50, -48, -52, -48, -50, -54, -54, -50, -46, -52, -50, -46, -50, -48, -46, -58, -52, -52, -48, -52, -44, -44, -50, -54, -48, -50, -54, -52, -50, -52, -52, -52, -46, -44, -52, -46, -48, -50, -50, -50, -54, -54, -48, -54, -48, -50, -50, -48, -44, -52, -50, -46, -50, -52, -46, -50, -48, -46, -48, -44, -50, -46, -50, -50, -46, -50, -42, -52, -48, -52, -52, -46, -52, -44, -50, -46, -54, -52, -50, -46, -48, -50, -48, -48, -48, -48, -48, -50, -50, -50, -50, -48, -52, -48, -50, -50, -50, -48, -52, -46, -50, -50, -46, -54, -48, -48, -50, -46, -50, -44, -46, -46, -46, -46, -48, -48, -52, -58, -54, -44, -48, -46, -50, -46, -52, -48, -48, -46, -54, -48, -50, -50, -44, -50, -48, -32, -48, -46, -50, -50, -48, -48, -46, -50, -48, -50, -54, -50, -52, -52, -48, -48, -48, -50, -52, -46, -46, -48, -50, -46, -50, -50, -46, -48, -50, -48, -42, -46, -52, -44, -52, -50, -50, -46, -50, -44, -54, -54, -48, -46, -44}.

References

[1] A. Rostovtsev. Changing Probabilities of Differentials and Linear Sums via Virtual Isomorphisms. Problems of Information Security. Computer Systems. No. 3, 50-60 (2009).

[2] A. Rostovtsev. Changing Probabilities of Differentials and Linear Sums via Isomorphism of Ciphers. International Association for Cryptologic Research. Cryptology e-print archive, report 2009/117, 2009 // available at http://eprint.iacr.org/2009/117.

[3] M. Kargopolov, Y. Merzlyakov. *Basis of Group Theory.* (Nauka, Moscow, 1982).

[4] M. Matsui. Linear Cryptanalysis Method for DES Cipher. In: *Advances in Cryptology — EUROCRYPT '93.* LNCS, vol. 765. (Springer-Verlag, 1994). P. 386–397.

[5] E. Biham, A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Advances in Cryptology — CRYPTO '90.* LNCS, vol. 537. (Springer-Verlag, 1991). P. 2–21.

[6] J.-C. Faugere. Groebner Bases. Applications in Cryptology. In: *FSE-metric converter ProductID07*, Luxemburg. Available at http://fse2007.uni.lu/slides/faugere

[7] H. Raddum, I. Semaev. New Technique for Solving Sparse Equation Systems. Cryptology e-print archive, report 2006/475, 2006 // Available at http: // e-print.iacr.org/2006/475.

[8] M. Albrecht, C. Cid. Algebraic Techniques in Differential Cryptanalysis. Cryptology e-print archive, report 2008/177, 2008 // Available at http: // e-print.iacr.org/2008/177.

[9] FIPS 197. Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[10] A. Biryukov, C. De Canniere, A. Braeken, B. Preneel. A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. *Advances in Cryptology – EUROCRYPT 2003.* LNCS, vol. 2556. (Springer-Verlag, 2003). P. 33−50.

[11] M. Atiyah, L. Macdonald. *Introduction to Commutative Algebra.* (Addison-Wesley, 1969).

[12] H. Heyes, S. Tavares. Substitution–Permutation Networks Resistant to Differential and Linear Cryptanalysis. Journal of cryptology. **9**, 1–19 (1996).